IPS Engine - Release Notes

Version 6.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 02, 2022
IPS Engine 6.4 Release Notes
43-640-772423-20220202

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Product integration and support **6**
Resolved issues **7**
Known issues **10**

Change log

Date	Change Description
2022-02-02	Initial release.

Introduction

This document provides the following information for the Fortinet IPS Engine 6.4 build 0114.

- Product integration and support on page 6
- Resolved issues on page 7
- Known issues on page 10

IPS Engine 6.4 build 0114 is a release to FortiGuard. It is not a built-in release for FortiOS 6.4.

For additional FortiOS documentation, see the Fortinet Document Library.

Product integration and support

The following table lists IPS engine product integration and support information:

FortiOS	6.4.0 and later

Resolved issues

The resolved issues listed do not list every bug that this release has corrected. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
580391	User cannot create MAC address-based policies in next generation firewall (NGFW) mode.
654356	Under NGFW policy mode, sessions are not revalidated when security policies change. **Workaround**: clear session after policy change.
662698	One-arm sniffer logging shows inaccurate SNMP application sent bytes.
672994	Web filter warning message does not contain certification chain.
676705	Custom IEC-104 app-ctrl signatures are skipped after signature database update.
677834	HTTP traffic is dropped when custom proxy options are applied to policy.
681611	IPS Engine crashes with 5.218 ips_dlp_alert.
683669	Firewall schedule settings do not follow daylight savings time.
688888	bzip2 including eicar is detected in the original direction of the flow mode firewall policy even though scan-bzip2 is disabled.
691196	One arm IPS URL filter cannot block HTTPS websites.
695441	User cannot get past block/override or warning page when doing a web filter override in flow mode.
695774	Remote category flow and proxy mode wildcard match differently.
696619	NGFW policy mode may block FortiGate Session Life Support Protocol (FGSP)-synced UDP sessions when asymmetric routing is used due to policy matching failure. Other traffic types such as TCP may also be affected in the case of failover of the reply-direction traffic to a different FortiGate in the FGSP cluster.
696753	Chassis multiple IPS Engine crashes and UTM web filter impact after enabling web filter content-header.
696819	IPS Engine archive timestamp dated from 1970.
707907	IPS Engine in flow deep inspection does not decrypt some TLS 1.3 session and causes problem with application control detection.
713068	FGSP support in NGFW policy mode.
715136	High memory usage for some slab objects.
718452	`set https-replacemsg disable` causes connection reset on URLs in URL filter list in flow inspection.

Bug ID	Description
719007	URL filtering followed by /* causes rating error.
719252	IPS Engine crashes.
721462	Memory usage increases to conserve mode after IPS Engine upgrade.
645848	FortiOS provides self-signed CA certificate intermittently with flow-based SSL certificate inspection.
678890	IPS engine stalls. Alarm clock crash occurs at `pat_search_nocase`.
687885	Inconsistent system performance with RFC2544 IXIA breaking point testing.
708941	High CPU while changing firewall policies.
709968	FortiGate drops UDP port 5440 traffic after rebooting both FortiGates.
712352	Firewall goes into conserve mode and IPS engine consumes high memory.
720605	URL filter with exemption may not avoid antivirus and IPS Engine inspection.
724400	facebook.com gives error in Firefox v89 with flow mode plus deep inspection.
728492	Chrome cannot load instagram.com without changing TLS PostQuantum Confidentiality from default to enabled.
729249	Web Filter categorizes private IP address/local URLs as newly observed domains.
730137	User cannot access website when the policy is in flow-based mode with web filter enabled.
735893	If running IPS Engine older than version 5.00246, 6.00099 or 7.00034, after the Chrome 92 update, FortiOS 6.2, 6.4 and 7.0 cannot reach specific websites in proxy mode with UTM applied. In flow mode, everything works as expected.
691338	Download drops to 0 kbps and slow website access after firmware upgrade.
721435	Download breaks when the policy is in flow mode with deep inspection and the NCP application is used on the host.
731459	In NGFW policy mode, disabling a security policy does not stop current traffic passing the firewall.
735893	Websites do not load in proxy mode after Chrome 92 update.
736906	The default `np-accel-mode basic` setting causes sporadic HTTPS deep inspection transaction failures with Application Control.
738144	The UTM function only works for a few seconds in GRE session.
741643	NGFW policy mode incorrectly blocks traffic or matches it to the wrong security policy.
744352	Websites open slowly in flow mode plus SSL deep inspection.
744888	FortiGate drops SERVER HELLO when accessing website using flow-based policy with deep SSL inspection.

Bug ID	Description
745163	ad.doubleclick.net cannot open in flow-mode with deep packet inspection and a security profile in Chrome.
754216	Flow mode web filter replacement message does not display using upstream proxy with HTTPS.
683066	IPS Engine crashes and consumes high CPU.
730235	FortiGate 5001E/5001E1 image build0202 (v7.0.2) ‘ipsengine’ application crashes during traffic testing.
752466	Deep inspection causes downloads to fail in ADVPN environment.
754579	Application performance is ten times worse when IPS Engine is applied in flow mode.
757122	Wildcard strings do not work as URL filter describes.
757951	CIFS oversize files cannot be blocked.
760555	[TAM/NTT-Com] Web filter UTM logs unexpected URL such as `url="https:///"`.
765859	Repeated IPS Engine signal 11 and signal 7 crashes.

Known issues

There are no known issues with this release of IPS engine version 6.4 for FortiOS.

To report a bug, please contact Customer Service & Support.